

Electronic payment method and transaction system supporting the use of digital currency

TECHNICAL FIELD

[001] The present invention relates to the technical field of electronic payment, and specifically to an electronic payment method supporting the use of digital currency.

BACKGROUND OF RELATED ART

[002] The theoretical study of digital currency has tended to be mature, but there still exist many factors such as a relatively high cost, which may restrict the application of digital currency. The payment scheme of digital currency is required to be compatible with the existing payment infrastructure to reduce the amount of modification as much as possible. However, the differences between digital currency and electronic currency may affect the compatibility design, which are mainly embodied in three points: Firstly, the underlying technology of digital currency generally adopts a decentralized mode, while the underlying technology of electronic currency generally adopts a centralized mode. Secondly, digital currency generally adopts a point-to-point mode between the user and merchant, while electronic currency generally adopts a four-party mode. Thirdly, digital currency is charged to the payee address of the merchant, while electronic currency is charged to a bank account of the merchant.

[003] When both electronic currency and digital currency are used for a payment, due to the differences in technology, the existing solution needs to provide different transaction media and transaction paths, which will generate an additional payment cost and reduce the reliability of the transaction system.

SUMMARY

- [004] According to one aspect of the present invention, an electronic payment method supporting the use of digital currency is provided. The method comprises: obtaining payee information from a transaction medium; wherein the payee information includes a first payee address stored in a first data field of the transaction medium and a second payee address stored in a second data field of the transaction medium; transmitting a first payment message to the first payee address and a second payment message to the second payee address based on a payment setting of a user; wherein the first payee address is an address at a first blockchain network and the second payee address is an address at a second blockchain network.
- [005] Optionally, the payee information further includes an electronic currency payee address, and the method further comprises transmitting an electronic currency payment message to the electronic currency payee address based on the payment setting.
- [006] Optionally, the first blockchain network is different from the second blockchain network.
- [007] Optionally, the first data field includes an identifier of the first blockchain network and the second data field includes an identifier of the second blockchain network.
- [008] Optionally, the payee information further includes a third payee address stored in a third data field of the transaction medium, and the third payee address is an address at a third blockchain network, and wherein the third blockchain network is a redundant network of the first blockchain network or the second blockchain network.
- [009] Optionally, the transaction medium comprises at least one of: barcode; two-dimensional code; non-contact tag; and non-transitory computer-readable storage medium.
- [010] Optionally, the transaction medium further stores digital currency header information including a flag bit, a first field for recording the amount of digital currency, and a second field for storing a check code of the header information.

[011] Optionally, the second field further includes: a first check code for checking the first payee address; a second check code for checking the second payee address; and/or a third check code for checking the third payee address.

[012] According to another aspect of the present invention, a transaction system supporting the use of digital currency is provided. The transaction system is configured to provide a transaction medium including a first data field and a second data field, wherein the first data field is used for storing a first payee address and the second data field is used for storing a second payee address; wherein the first payee address is an address at a first blockchain network and the second payee address is an address at a second blockchain network; obtain a payment setting via a payment application of a user; provide a transaction route to transmit a first payment message to the first payee address and transmit a second payment message to the second payee address.

[013] Optionally, the transaction medium further includes an electronic currency payee address, and the transaction system is further configured to transmit an electronic currency payment message to the electronic currency payee address based on the payment setting.

[014] Optionally, the transaction system is further configured to provide a first transaction route directed to the first payee address; provide a second transaction route directed to the second payee address.

[015] Optionally, the transaction system is further configured to provide a third transaction route directed to a third payee address, wherein the third payee address is an address at a third blockchain network, and the third blockchain network is a redundant network of the first blockchain network or the second blockchain network.

[016] The electronic payment method supporting the use of digital currency provided herein distributes multiple payee addresses corresponding to different blockchain networks in the same transaction medium, and can perform the transmission of digital currency according to the user setting. This method can reduce the transaction cost, improve the user experience

and further promote the popularization of digital currency. The transaction system supporting the use of digital currency provided herein is low in the deployment cost and may guarantee the reliability of the transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[017] FIG. 1 is a flow diagram of an electronic payment method supporting the use of digital currency, according to one embodiment of the present invention.

[018] FIG. 2 illustrates a transaction medium, according to one embodiment of the present invention.

[019] FIG. 3 illustrates a network topology of a transaction system supporting the use of digital currency.

[020] FIG. 4 illustrates another network topology of a transaction system supporting the use of digital currency.

DETAILED DESCRIPTION

[021] Specific details are set forth in the following description in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the embodiments of the present invention may be implemented without these specific details. In the present disclosure, specific numbers references may be made, such as a first element, a second device, etc. However, the specific numerical references should not be understood as being subject to their literal order, but should be understood as meaning that the first element is different from the second element.

[022] The specific details set forth in the present disclosure are merely exemplary, and the specific details may be varied, but still fall within the spirit and scope of the present invention. The term "coupling" is defined as being directly connected to a component or indirectly connected to the component via another component. The term "transaction route" refers to the route from a user to a payee (merchant), which includes determining the best path from the user to the payee and enabling the transmission of

information via the network.

[023] Preferred embodiments for implementing the methods, systems and devices of the present invention are described below by reference to the drawings. Although various embodiments are described with respect to a single combination of elements, it should be understood that the present invention encompasses all possible combinations of the elements. That is, if one embodiment includes elements A, B and C, and the second embodiment includes elements B and D, the present invention should also be considered as including other remaining combinations of A, B, C or D, even if not specifically disclosed.

[024] As shown in FIG. 1, one embodiment of the present invention provides an electronic payment method supporting the use of digital currency, including steps S10-S15.

[025] Step S10: obtain payee information from a transaction medium.

[026] In this step, the payee information may be obtained from a transaction medium via scanning or a non-contact manner (e.g., based on near-field communication technology) by a payment application installed on the user's smartphone. The payee information includes a first payee address stored in a first data field of the transaction medium and a second payee address stored in a second data field of the transaction medium. The first and second payee addresses may belong to different payee addresses of the same payee, or may be the respective payee addresses of different payees.

[027] The user may pay digital currency to the first and second payee addresses, and may enable a payment using electronic currency in parallel with digital currency. Specifically, the first payee address may be an address at a first blockchain network and the second payee address is an address at a second blockchain network, wherein the first blockchain network is different from the second blockchain network. As one example, the first blockchain network is a Bitcoin network, and the second blockchain network is an Ether network. As another example, the first blockchain network and the second blockchain network are different

subnets of the same blockchain network, or the first and second blockchain networks support different blockchain protocols, respectively. To distinguish between the different blockchain networks, an identifier of the first blockchain network is stored in the first data field, and an identifier of the second blockchain network is stored in the second data field. For example, an identifier occupies 3bit. The identifier BTC of the first blockchain network indicates that the first blockchain network is the Bitcoin network, and the identifier ETH of the second blockchain network indicates that the second blockchain network is the Ether network.

[028] According to some embodiments of the present invention, the transaction medium may comprise barcode, two-dimensional code, non-contact tag and other non-transitory computer-readable storage media (e.g., flash memory, mobile hard disk), etc. Herein, the two-dimensional code is taken as an example to illustrate below. The two-dimensional code includes two data fields, wherein the first payee address is stored in the first data field and the second payee address is stored in a second data field. By scanning the two-dimensional code, the user may get two different payee addresses of the payee. The two-dimensional code may further include a third data field, wherein a third payee address is stored in the third data field and the third payee address is an address at the third blockchain network. In some modified embodiments, the third blockchain network may be a redundant network of the first blockchain network or the second blockchain network. As such, when the first or the second blockchain network breaks down, the third blockchain network may take over the work of the fault network, which in turn guarantees the reliability of the transaction.

[029] As a further modification, multiple payee information and digital currency header information may be stored in the transaction medium. As shown in FIG. 2, the electronic currency payee information 11 and digital currency payee information 12 are both stored in the transaction medium. They can be used for electronic currency payment and digital currency payment, respectively. The digital currency payee information 12 includes

digital currency header information 120, the first payee address 121, the second payee address 122 and the third payee address 123. The digital currency header information 120 includes a header information flag bit, a first field for recording the total amount of digital currency, and a second field for storing a check code of the header information. Preferably, the second field further includes a first check code, a second check code and a third check code. The first, second and third check codes are used for checking the first payee address, the second payee address and the third payee address, respectively. The checking methods may include the cyclic redundancy check, the MD5 check, etc.

[030] Step S15: transmit a first payment message to the first payee address and a second payment message to the second payee address based on the payment setting of a user.

[031] At the step, a smartphone may obtain the payment setting of a user. For example, the user wants to divide the payment amount in order to use their own different payer addresses (digital currency accounts) in different blockchains to pay accordingly. In addition, the user may also want to use electronic currency to pay a portion of the payment amount. The user may make respective payment setting or selection by the payment application installed on the smartphone. Therefore, the payment application may transmit the first payment message to the first payee address according to the payment setting of the user to pay a first amount of digital currency, and transmit a second payment message to the second payee address to pay a second amount of digital currency. In some cases, the first payment message enables an unconditional payment, while the second payment message may be bound with certain payment condition (e.g., exchange rate, prohibitive amount, transaction day or the like), thereby providing flexibility in the payment. In some cases, the first and second payment messages may include the confirmation messages about this transaction. After obtaining a feedback of the confirmation message from the payee, the payment of digital currency will be executed. In the case when the user expects to use electronic currency, the smartphone transmits an electronic

currency payment message to the electronic currency payee address (e.g., electronic currency payee information 11 as shown in Fig. 2) for paying electronic currency. The payment of electronic currency and the payment of digital currency may be performed in parallel. The electronic currency payee address may be independent of a blockchain network. It can be a bank account, an account of a payment application, or a payee address at the third-party platform, etc, of the payee.

[032] In some embodiments of the present disclosure, the transaction route may be determined according to the user setting or state of the blockchain network, including determining the payment of a first amount of digital currency to the first payee address via a first transaction route (directed to or through the first blockchain network), and the payment of a second amount of digital currency to the second payee address via a second transaction route (directed to or through the second blockchain network). In the case when the first transaction route or the second transaction route is found to be blocked, a third transaction route (directed to or through the third blockchain network being a redundant network) may be determined to pay a third amount of digital currency to the third payee address. The duty of determining the route may be performed by a router or switch that accesses a payment network connecting each blockchain network.

[033] The electronic payment method supporting the use of digital currency provided herein can achieve the technical effects as follows.

[034] 1. The merchant is able to set up multiple payee account information and multiple payee addresses located on different blockchains supporting electronic/digital currency on the same transaction medium. 2. Users can select different routes for transactions via a payment application, and can select different payment methods, designate a respective electronic/ digital currency account for payment, which improves the user experience. 3. It is helpful to reduce the transaction cost and guarantee the reliability of the transaction and promote the popularization of digital currency.

[035] It should be understood that the steps S10, S15 of the electronic payment method described above can be divided, combined or inserted

with one or more other sub-steps therebetween. Based on the foregoing disclosure, those skilled in the art can foresee various implementations with simple modifications. As long as the implementations are capable of achieving the above technical effects, they all should fall within the protection scope of the present invention.

[036] The present invention also provides a transaction system supporting the use of digital currency. The transaction system can be configured to provide a transaction medium and a transaction route to facilitate users to pay respective digital currency to different payee addresses located at the blockchain network(s). The transaction medium and the transaction route are generated per transaction, and the transaction route can be changed in the transaction process. As an example, the transaction medium may be a data packet transmitted from a merchant to a user via NFC (near field communication) technology. The data packet includes a first data field and a second data field that are independent of each other, wherein the first data field is used for storing a first payee address, and the second data field is used for storing a second payee address. The first and second payee addresses are an address at the first blockchain network and an address at the second blockchain network, respectively. Thus, the payment user may transmit payment messages to different addresses of the same payee (merchant), including paying the respective digital currency.

[037] In some embodiments, the transaction system communicates with the smartphone held by the user in order to obtain a payment setting of the user. The transaction system may also be configured to provide a first transaction route directed to the first payee address and a second transaction route directed to the second payee address to facilitate using digital currency to pay. Preferably, based on the payment setting of the user, the transaction system may provide a digital currency payment method that conforms to the user intention by configuring the first transaction route and the second transaction route. For example, a first payment message can be transmitted via the first transaction route, and a second payment message can be transmitted via the second transaction

route. The union of the first payment message and the second payment message corresponds to information of the digital currency that the user expects to pay.

[038] In some embodiments, the transaction medium includes an electronic currency payee address. In that case, the transaction system transmits an electronic currency payment message to the electronic currency payee address based on the payment setting of the user, thus enabling a payment using electronic currency in parallel with digital currency. The electronic currency payment message may include electronic currency, coupons, discount rates, etc. Since the electronic currency payee address and the digital currency payee address are stored in the same transaction medium, the user can conveniently use electronic currency in parallel with digital currency to pay, which not only increases the usage rate of the transaction medium, but also improves the user experience.

[039] As shown in FIG. 3, the shown transaction system includes two blockchain networks, Net1 and Net2, which support different blockchain protocols, respectively. The first blockchain network Net1 includes a plurality of nodes N1, each of them is coupled to each other, wherein one of the nodes N1 corresponds to the first payee address Adr1. Similarly, the second blockchain network Net2 includes a plurality of nodes N2, wherein one of the nodes N2 corresponds to the second payee address Adr2. The first payee address Adr1 and the second payee address Adr2 are the payee addresses of the same merchant located at different blockchain networks. Thus, the user may pay a first amount of digital currency to the first payee address and pay a second amount of digital currency to the second payee address according to his/her intention during the transaction.

[040] FIG. 4 illustrates another network topology of a transaction system supporting the use of digital currency. FIG. 4 includes three blockchain networks Net1, Net2 and Net3, which include a plurality of nodes coupled to each other. Specifically, one node N1 of the first blockchain network Net1 has a first payee address Adr1, and one node N2 of the second blockchain network Net2 has a second payee address Adr2, and one node

N3 of the third blockchain network Net3 has a third payee address Adr3. The first blockchain network Net1 and the second blockchain network Net2 are connected to each other in parallel. The third blockchain network Net3 is implemented as a redundant network of the second blockchain network Net2.

[041] The transaction system provides different transaction routes 211, 221, which are directed to the first payee address Adr1 and the second payee address Adr2 of the merchant, respectively. The third blockchain network Net3 may adopt the same consensus algorithm as that of the second blockchain network Net2 and replace the second blockchain network Net2 in case it could break down. Accordingly, the transaction system provides another transaction route 231, which is directed to the third payee address of the merchant, which is an address at the third blockchain network Net3. The transaction route 221 and transaction route 231 may at least partially overlap to reduce the cost of routing or deploying the lines.

[042] In some modified embodiments, the routing of the transaction system may be implemented by one or more router(s) or switch(s) (not shown in the figures) connected to the system. Specifically, the router may not only select the suitable transaction route 211, 221, 231 per the payment setting of the user, but also may measure the state of each blockchain network, and further switch between the transaction routes according to the state of each blockchain network.

[043] In some embodiments, a supervising node is disposed on the second blockchain network Net2. The node may supervise the work state of the second blockchain network. When the route going through the second blockchain network is found to be blocked, one router connected to the supervising node can select the third transaction route 231 going through a third blockchain network. The router may forward the payment message, which would otherwise go through the second transaction route 221, to the third transaction route 231 for transmission. In some embodiments, the transaction system and the smartphone held by the user may utilize the digital currency header information stored in the transaction medium to

check the first payee address and the second payee address, respectively. The checking that is performed at the end of the transaction system may be performed by a router on the supervising node or a processor coupled thereto.

[044] The present disclosure provides a machine-readable storage medium, on which a plurality of computer-executable instructions can be stored. The computer-executable instructions, when executed by a processor, may implement the electronic payment method as described above.

[045] It should be understood that, a mobile payment device held by the user, such as a smart phone, falls within the protection scope of the present invention. The mobile payment device comprises a memory, a processor and a computer program stored on the memory and executed by the processor, etc. The processor, when executing the computer program, may implement each step of the electronic payment method as described above.

[046] In some embodiments, at least a part of the system can be implemented by using a set of distributed computing devices connected by a communication network, or implemented based on a "cloud" system. In the system, the multiple computing devices operate together to provide services by using the shared resources. The cloud-based implementation may provide one or more advantages, including openness, flexibility and scalability.

[047] Those skilled artisans will understand that, various descriptive logical blocks, modules, circuits and the steps of methods described in connection with the aspects disclosed herein can be implemented as electronic hardware(s), computer software(s), or a combination thereof. In order to demonstrate the interchangeability between the hardware and the software, various descriptive components, blocks, modules, circuits and steps have been generally described in terms of their functionality. However, whether the disclosed functionality is implemented as hardware or software will depend upon the particular application and the design constraints applied to the overall system. Those skilled in the art may choose to implement the functionality in a variable manner, which may depend on the particular

application. Note that any decisions on the implementations should not be interpreted as departing from the scope of the present invention.

[048] The foregoing description is only for the preferred embodiments of the present disclosure, and is not intended to limit the protection scope of the present invention. Various modifications can be made by those skilled in the art without departing from the spirit of the present invention and the claims.

What is claimed is:

1. An electronic payment method supporting the use of digital currency, comprising:

obtaining payee information from a transaction medium; wherein the payee information includes a first payee address stored in a first data field of the transaction medium and a second payee address stored in a second data field of the transaction medium;

transmitting a first payment message to the first payee address and a second payment message to the second payee address based on a payment setting of a user;

wherein the first payee address is an address at a first blockchain network and the second payee address is an address at a second blockchain network.

2. The method of claim 1, wherein the payee information further includes an electronic currency payee address,

the method further comprises:

transmitting an electronic currency payment message to the electronic currency payee address based on the payment setting.

3. The method of claim 1, wherein the first blockchain network is different from the second blockchain network.

4. The method of claim 1, wherein the first data field includes an identifier of the first blockchain network and the second data field includes an identifier of the second blockchain network.

5. The method of any one of claims 1 to 4, wherein the payee information further includes a third payee address stored in a third data field of the transaction medium, and the third payee address is an address at a third blockchain network, and wherein the third blockchain network is a redundant network of the first blockchain network or the second blockchain network.

6. The method of claim 5, wherein the transaction medium comprises at least one of:

barcode;
two-dimensional code;
non-contact tag; and
non-transitory computer-readable storage medium.

7. The method of claim 5, further comprising:

determining a first transaction route for paying a first amount of digital currency to the first payee address; and/or

determining a second transaction route for paying a second amount of digital currency to the second payee address.

8. The method of claim 7, further comprising:

determining a third transaction route to pay a third amount of digital currency to the third payee address when the first transaction route or the second transaction route is blocked.

9. The method of claim 5, wherein the transaction medium further stores digital currency header information including a flag bit, a first field for recording an amount of digital currency, and a second field for storing a check code of the header information.

10. The method of claim 9, wherein the second field further includes:

a first check code for checking the first payee address;

a second check code for checking the second payee address; and/or

a third check code for checking the third payee address.

11. A transaction system supporting the use of digital currency, configured to:

provide a transaction medium including a first data field and a second data field, wherein the first data field is used for storing a first payee address and the second data field is used for storing a second payee address; wherein the first payee address is an address at a first blockchain network and the second payee address is an address at a second blockchain network;

obtain a payment setting via a payment application of a user;

provide a transaction route to transmit a first payment message to the first payee address and transmit a second payment message to the second

payee address.

12. The transaction system of claim 11, wherein the transaction medium further includes an electronic currency payee address,

the transaction system is further configured to transmit an electronic currency payment message to the electronic currency payee address based on the payment setting.

13. The transaction system of claim 11, further configured to:
provide a first transaction route directed to the first payee address;
provide a second transaction route directed to the second payee address.

14. The transaction system of claim 11, further configured to:
provide a third transaction route directed to a third payee address,
wherein the third payee address is an address at a third blockchain network, and the third blockchain network is a redundant network of the first blockchain network or the second blockchain network.

15. The transaction system of any one of claims 11 to 14, further configured to check the first payee address and the second payee address by using digital currency header information stored in the transaction medium.

16. A machine-readable storage medium storing a plurality of computer-executable instructions thereon,

wherein the computer-executable instructions are configured to, when executed by a processor, implement the method of any one of claims 1 to 10.

17. A mobile payment device, comprising a memory, a processor and a computer program stored in the memory and executed by the processor, wherein the processor is configured to, when executing the computer program, implement each step of the method of any one of claims 1 to 10.